Cybersecurity: Vom Hype in die Integration

Know-how Zum Jahreswechsel ziehen auch Cybersecurity-Reseller gerne Resumé und stellen sich die Frage, mit welchen Themen sie im nächsten Jahr und mittelfristig Geld verdienen werden.

Von Andrew Campbell

Gerade im Cybersecurity-Bereich gehen Technologien oft schon im Jahresverlauf vom Hype in die Integration in eine grössere Suite über und die Frage nach Trends ist, ähnlich wie in der Mode, oft irrelevanten Einflüssen ausgesetzt.

Eine Betrachtung der für 2018 relevanten Themen sollte sich entlang der bekannten offenen Fragen bewegen: Was wird angegriffen? Wie wird angegriffen? Warum sind Angriffe oft erfolgreich? Es überrascht jedenfalls nicht, dass es die Angreifer auf die Daten abgesehen haben, welche sich entweder durch den Weiterverkauf oder deren vermeintlich rückgängig zu machende Zerstörung mittels Verschlüsselung-Ransomware zu Geld machen lassen.

Generell gilt hier allerdings: Wer Angriffsfläche preisgibt, wird angegriffen. Wer es dem Angreifer einfach macht, wird eher angegriffen. Angreifer haben dank AWS & Co. sehr kostengünstig Zugriff auf effektiv unlimitierte Compute-Power, KI und Storage und wissen diese einzusetzen. Mittlerweile gibt es keine Firma mehr, die nicht als Ziel qualifiziert ist. Das archetypische Ein-Frau/Mann-Schweizer-KMU ist dabei durchaus sehr beliebt. Welche Bereiche sind also für 2018 und in Zukunft von Bedeutung?

Endpunkt

Aufgrund der sich stets verändernden Definition von Arbeitsgerät und Infrastruktur rückt der Endpunkt noch weiter in den Fokus. Endpunkte kommen in allen Farben und Formen vor. Nicht nur das Smartphone oder der Laptop sind hiermit gemeint: Endpunkte können auch Server, Kassensysteme, Industrie-PCs wie auch das kleine IoT-Gerät sein. Erfolgsversprechende Lösungsansätze berücksichtigen, dass auf der einen Seite Ressourcen und bei Smartphones und IoT sogar Energie knapp sind, während die Anforderungen an Sicherheitslösungen ein um Faktoren höheres Schutzbedürfnis darstellen als bisher – dies aufgrund der immer genauer auf einzelne Ziele abgestimmten Angriffe und der teilweise (lebens-) kritischen Prozesse, für welche diese Endpunkte zuständig sind.

Welchen spezifischen Eigenschaften und Determinanten eines Cybersecurity-Produkts sollte ein Anbieter heute besonderes Augenmerk schenken – und notabene auch seine bestehenden Produkte darauf hin überprüfen? Regelmässige Scans, viele einzelne Prozesse, welche dauernd die Systemtätigkeiten überwachen und belasten, aber auch Signaturen, welche regelmässig heruntergeladen werden müssen und die Basis für den Schutz darstellen, sind in Zeiten von einfach und automatisiert veränderbarer Malware nicht mehr wirkungsvoll.

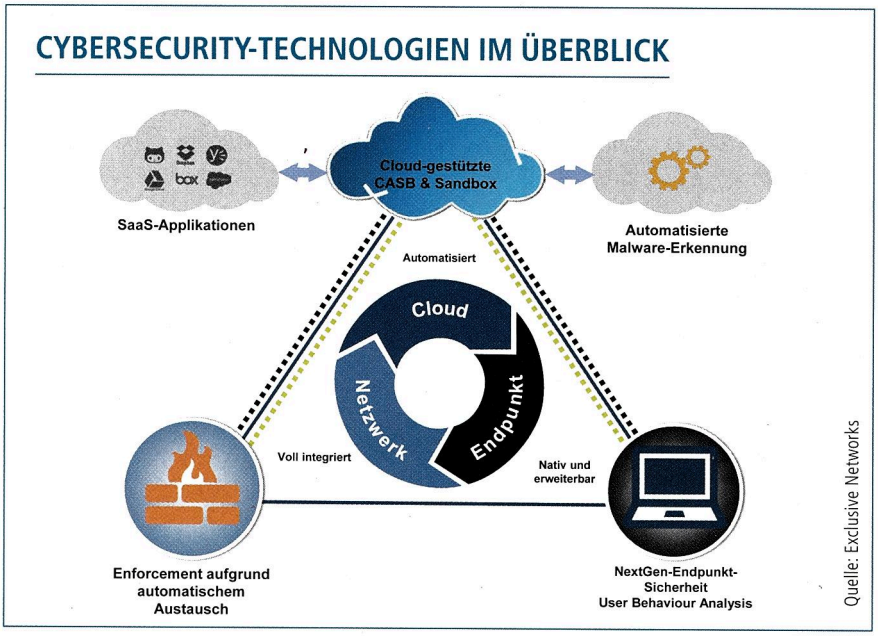
Eine zeitgemässe Lösung sollte schlicht diejenigen Techniken erkennen, die der Angreifer benützt, um den Angriff erfolgreich zu machen – sie muss also auch vor noch unbekannten Angriffen schützen und deren Ausführung verhindern können. Wenn so vorgegangen wird, macht es auch keinen Unterschied mehr, ob der Angriff äusserst genau auf das Ziel abgestimmt ist oder weltweit per Giesskannen-Prinzip verteilt wird. Erkennt ein Endpunkt dank vorgelagerter, KI-gestützter Vorarbeit auf der Basis von Millionen von Artefakten auch ohne Internetverbindung, aber mit hohem Verlässlichkeitsgrad, extrem kleiner Latenz und geringem Energieaufwand, ob eine ausführbare Datei für den Endpunkt schädlich sein wird, dann sprechen wir von echter Next-Gen Endpoint Security.

Ebenso ist die Vorgehensweise, das Rendering von Dokumenten in eine sichere Zone auszulagern und nur noch die visuelle Darstellung an den Endpunkt zu übertragen, interessant und bei hoher Interaktionsdichte mit externen Dokumentquellen unbedingt als Erweiterung des bestehenden Dispositivs in Betracht zu ziehen.

Koppelt man diese beiden Technologien mit UBA – User Behaviour Analytics – wird auch der authentisierte Endpunkt, der von einem kompromittierten Insider oder einem Dritten gesteuert wird, zuverlässig von wertvollen Daten ferngehalten, da die Identifizierung auffälliger Aktionen, welche üblicherweise unter dem Radar bleiben würden, immer ausserhalb normaler Verhaltensmuster läuft und diese durch die Methode erkannt werden können.

Sicherung von Off-Site-Datennutzung

Im Channel ist man sich seit einigen Jahren bewusst, dass Compute Loads und



Von der Cloud übers lokale Netzwerk bis hin zum Endpunkt: Sicherheitslösungen sollten heute vielschichtig sein.

Storage längerfristig und nachhaltig den Weg in die Cloud angetreten haben. Nur sehr wenige Firmen schaffen es, sich komplett von XaaS-Angeboten, spezifisch der Einstiegsdroge SaaS, fernzuhalten. Sehr schnell sind ein paar nutzbringende Dienste mal im Freemium-Modell bezogen und werden in der Firma erst einmal als Schatten-IT genutzt, bis sie per «fait-accompli» über Nacht als offizieller Teil von produktiven Prozessen genutzt werden und sogar Geld dafür gezahlt wird. Ähnlich verhält es sich mit IaaS: Meist werden in nicht-sanktionierter Art Compute Loads testhalber ausgelagert, bis Anwendungen gefunden werden, die sich sonst nicht kostengünstig betreiben lassen – und voilà, haben diese IaaS-Dienste bereits den Weg in die Firma gefunden. Die abschliessende Adoption und Bewegung Richtung Cloud geht dann meist über «Cloud Light»-Hybrid-Ansätze bis zur kompletten Auslagerung.

Wo bleiben hier die Daten und insbesondere die Umsetzung der normalerweise strengen Richtlinien und Sicherheitsdispositive in der Cloud? Vielfach auf der Strecke.

Dank der Cloud ist es so einfach wie attraktiv, Kollaboration einzurichten. Es ist noch einfacher, Daten zu teilen – ein Klick genügt. Was in der Praxis passiert ist jedoch, dass Cloud-artig Reverse Privilege Escalation erlebt wird: Was mal geteilt wurde, wird nicht mehr zurückgenommen. Niemand schaut so genau, was da geteilt wird und in welche Richtung. Firmen machen sich hier ein neues Daten-Scheunentor auf und haben oft keine Übersicht oder Kontrolle über beispielsweise die Dateien, welche von Drittparteien auf diese geteilten Arbeitsbereiche gelegt werden. Am schlimmsten zu bewerten ist menschliches Versagen à la «Teilen mit allen…global».

Eine für die Cloud gedachte Lösung zur Sicherung der Daten muss zwangsweise ebenfalls in der Cloud leben. In Kooperation mit den SaaS-Anbietern sollte sichergestellt werden, dass man den Gedanken des DLP ins SaaS-Zeitalter mitnimmt.

Das eingesetzte Produkt weiss und kontrolliert, welche Dateien – idealerweise mit welcher Klassifizierung – wann von wem mit wem wie lange geteilt wurden und verhindert, wo nötig, deren Ablage oder Nutzung. Falls unbekannte Dateien von aussen beziehungsweise von Nicht-Mitarbeitern auf den Kollaborationsflächen auftauchen, werden diese zuerst auf schädlichen Inhalt geprüft und erst dann überhaupt internen Mitarbeitern freigegeben. Das Produkt soll sich mit allen grossen SaaS-Anbietern verstehen und so sicherstellen, dass eine Sicherheits-Baseline für alle Dienste gilt – mit einem Klick durchgängig und gleich konfiguriert. Bei erhöhtem Bedarf an Sicherheit oder Compliance-getriebenem Zwang können solche Lösungen auch die transparente Off-Site-Verschlüsselung der Daten in der Cloud übernehmen, damit auch bei Kompromittierung der Cloud selbst die Integrität und der Schutz der Daten gewährleistet bleibt.

Automation, Big Data, KI

Firmen sind immer weniger in der Lage, sich Teams in der Grösse zu leisten, welche für den Betrieb und die Überwachung notwendig wären, um eine nachhaltige Sicherheit zu gewährleisten. In Schweizer KMU sieht die Situation oft prekär aus: Häufig wird die Aufgabe «Sicherheit» nicht von einer Fachperson, sondern in Personalunion zum Beispiel vom Geschäftsführer selber wahrgenommen. Eine Rolle, die angesichts der vielen damit verbundenen Zugriffsrechte verständlich ist, mit der man sich aber gerade dadurch erhöhten Gefahren aussetzt. Es kann gefährlich ausgenutzt werden, wenn der Rolleninhaber kompromittiert wird – und dies ist ziemlich wahrscheinlich, weil ihm die Fachkompetenz typischerweise fehlt. Angreifer haben, wie erwähnt, maximale Automation und Ressourcen zur Verfügung. Dies steht in starkem Kontrast zu denen, die abwehren müssen.

Sicherheit muss automatisiert und vereinfacht werden. Firewalls in einem IaaS-Kontext sollten in einem Pay-as-you-go-Modell konsumierbar werden. Produkt, Lizenz, Services und Support können dabei im Minutentakt, orchestriert durch Frameworks und deren Feeds aus der Cloud, ebenfalls in der gleichen Rate erneuert werden. Security Services sind auf den grösseren IaaS-Plattformen bereits konsumierbar erhältlich und helfen, IT-Betriebskosten deutlich zu senken.

Die anfallenden Daten kann sich kein Mensch mehr über eine analoge Schnittstelle zu Gemüte führen. Insbesondere Angriffe und Anomalien der subtileren Art können nicht mehr manuell abgehandelt werden. Hier braucht es die Kraft von Big Data, um mit den Datenmengen zurechtzukommen und insbesondere auch die Intelligenz von neuen KI-Ansätzen, um aus den Milliarden von Log-Zeilen einen Angriff herauszulesen und über offene Schnittstellen beispielsweise Firewalls anzuweisen, gewisse Verbindungen zu stoppen. Es kann heute oft nicht mehr gewartet werden, bis ein Mensch sich mit einer Sache beschäftigt hat: Kosten und Bandbreite stehen in keinem Verhältnis zu den Ressourcen und den sehr zeitnah bis unmittelbar nötigen Schritten zur Remediation beziehungsweise Abwehr.

Im Rahmen der Automatisierung kommt einem Faktor eine äusserst wichtige Rolle zu: die automatisierte Verringerung der Angriffsfläche durch dauerndes Scannen auf Sicherheitslücken und Vulnerability Management. Nur so können die Schwachstellen, welche oft durch rein menschliches Verhalten offenbleiben – sei es das Nicht-Handeln der Verantwortlichen oder das Fehlen von Personen, die das Prüfen durchführen –, automatisiert aufgezeigt und geschlossen werden. Idealerweise hat eine solche Lösung Schnittstellen, welche eine ebenfalls automatisierte Remediation der Sicherheitsrisiken ermöglicht.

Fazit

Schweizer Cybersecurity-Reseller verdienen auf mittlere bis lange Sicht gute Margen, wenn sie ihre Angebote um Dienstleistungen ergänzen, welche ihren Kunden helfen, ihre Daten und Prozesse mit Konzentration auf die wichtigen Themenkreise Endpunkt und Cloud Access zu schützen.

Endkunden möchten immer mehr den One-Stop-Shop mit einem Ansprechpartner, der zur Verantwortung gezogen werden kann. Es ist wie mit der lokalen Autogarage, bei der man sein Fahrzeug routinemässig vorbeibringt und dabei feststellt, dass man schon etliche tausend Kilometer mit einem undichten und damit unsicheren Bremssystem gefahren ist – wenn man Glück hat. Im Worst Case fährt man gegen die Wand. In dieser Analogie weitergedacht sind Angebote, welche wir heutzutage mit hohem gefühlten Wert assoziieren, solche, die Over-the-Air neue Funktionen einspielen und bei Problemen aufgrund einer andauernden Telemetrie sehr schnelle Reaktionen zulassen, bevor gravierende Folgen auftauchen. Was in der Industrie schon seit längerem umgesetzt und erwartet wird, ist nun ein Potentialfeld für Reseller in der IT Security.

Diese neuen Dienstleistungen sollten auf der Basis von Produkten geschehen, welche den Fokus auf die Verhinderung eines erfolgreichen Angriffes legen. Dies führt systemisch gesehen schon zu Produkten, welche der fortschreitenden Automation der Angreifer gerecht werden. Idealerweise findet dieses Enforcement nicht über eine fragmentierte Systemlandschaft statt, sondern so integriert wie möglich. Herstellerplattformen und Technologie-Allianzen sollten bei der Auswahl dieser Lösungen Vorrang haben. Die Verantwortung für eine abgestimmte und durchgehende Sicherheit darf nicht beim Admin liegen, sondern sollte vielmehr beim Hersteller und in seiner Kernkompetenz sein. ■

DER AUTOR

Andrew Campbell ist seit 2014 als Head Business Development und Marketing bei Exclusive Networks tätig, wo er das Business Development der führenden Cybersecurity-Brands verantwortet.